DigitalCitadel™ User Manual

PERSONAL

DigitalCitadel™

PERSONAL

IDSS INTELLIGENT DIGITAL SECURITY SOLUTIONS LLC

©2015 Intelligent Digital Security Solutions, LLC
9187 Clairmont Mesa Blvd., Suite #6629,
San Diego, CA 92123. All rights reserved.
All trademarks are the property of IDSS.

DigitalCitadel™ PERSONAL Table of Contents

About This User Guide 3

System Requirements 3

Recommendations 3

Setup 4

Device Initialization 5

Device Usage 8

Device Options 9

DC Settings 10

Browse DC 10

Format DC 10

Online Support 10

About DC 11

Shutdown DC 11

Drive Letter Conflict 12

About This User Guide

This user manual covers the **IDSS Digital Citadel™** (referred to simply as **DC** from this point forward) based on the factory image with no implemented customizations.

System Requirements

PC Platform

- Pentium III (or faster) processor equivalent
- 15MB free disk space
- USB 2.0/3.0 port
- Two consecutive drive letters after the last physical drive*

PC Operating System Support

- Windows® 7
- Windows® Vista Sp2
- Windows® 8/8.1 (RT not supported)

Recommendations

To ensure there is ample power provided to the **DC** device, insert it directly into a USB port on your notebook or desktop, as seen in ***Figure 1.1***. Avoid connecting the **DC** to any peripheral device(s) that may feature a USB port, such as a keyboard or USB-powered hub, as seen in ***Figure 1.2***.

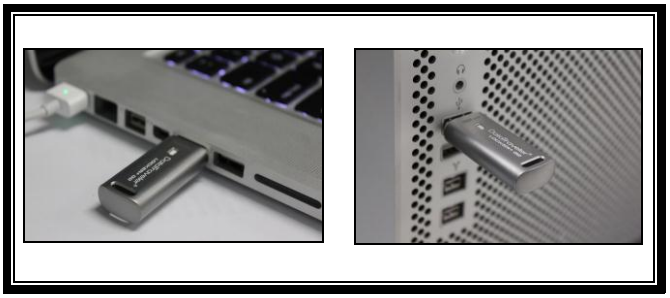

Figure 1.1 – Recommended Usage

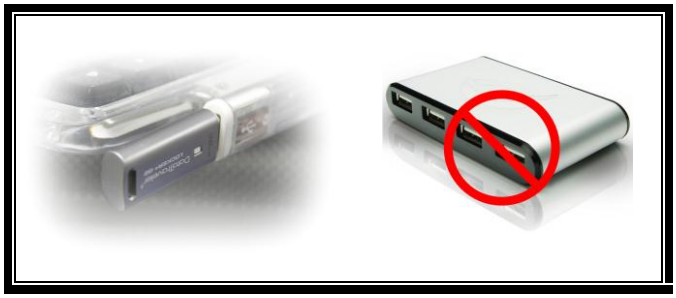

Figure 1.1 – Not Recommended

*Note: See 'Drive Letter Conflict' on **page 12**.

Setup

1. Insert the **DC** into an available USB port on your notebook or desktop and wait for Windows to detect it.

   - Windows Vista/7 users will receive a device driver notification as seen in ***Figure 2.2***.

Figure 2.1 – Found New Hardware

Once the new hardware detection is complete, windows will begin the initialzation process.

   - If the Windows autorun function is enabled, you can skip the next step and go to page 5 - **Device Initialization.**

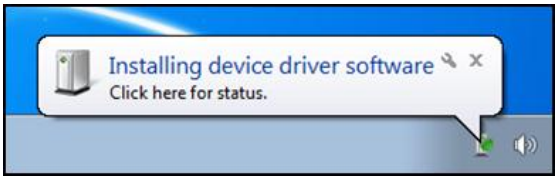

Figure 2.2 – Device Driver Installation (Windows Vista/7)

   - If the Windows autorun function is disabled, as it is in Windows 7 by default, you may see an AutoPlay window similar to the one in ***Figure 2.3***.

2. Select the option *'Run DC_Launcher.exe'*.

AutoPlay
DVD RW Drive (K:) DC
Always do this for software and games:
Install or run program from your media
Run DC_Launcher.exe
Published by Intelligent Digital Security Solutions
General options
Open folder to view files
using Windows Explorer
View more AutoPlay options in Control Panel

Figure 2.3 – AutoPlay Window (Windows Vista/7)

If Windows does not AutoPlay, simply browse to the DVD-RW partition (***Figure 2.4***) and manually execute the DC_Launcher program. This will also start the initialization process.

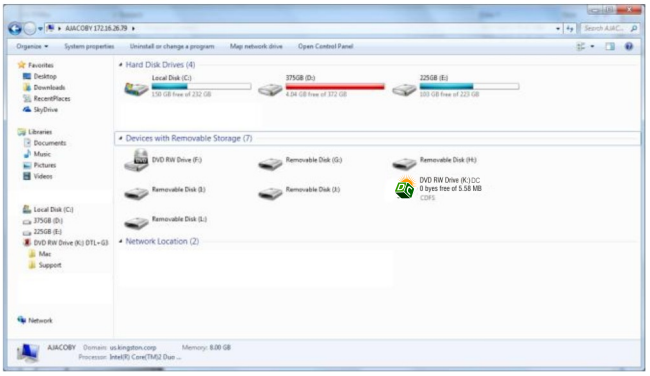

Figure 2.4 – DC Contents

(Note: Menu options in the AutoPlay window may vary depending on what programs are currently installed on your computer. If enabled, AutoRun will start the initialization process automatically.)

Device Initialization

1. Review the license agreement and click 'Next' (***Figure 3.1***). (Note: You must accept the license agreement before continuing; otherwise, the 'Next' button will remain disabled.)

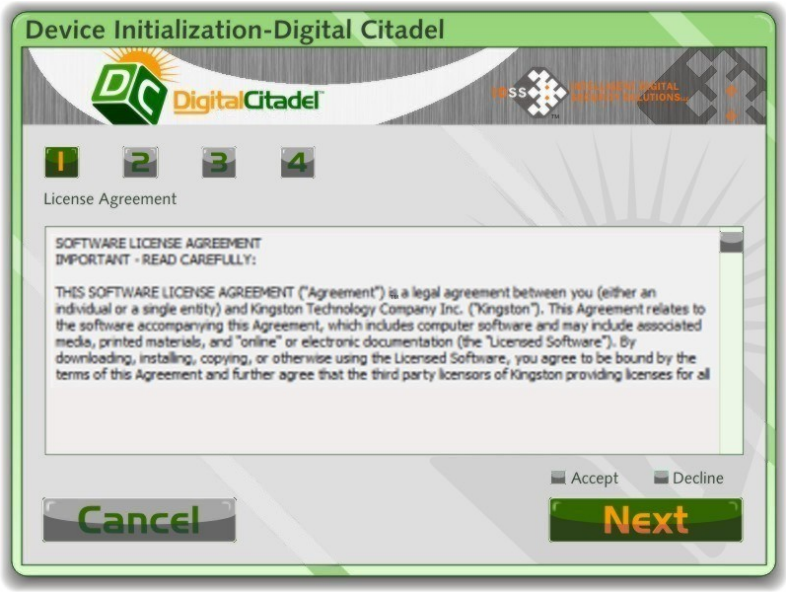
Device Initialization-Digital Citadel
DigitalCitadel
1
2
3
4
License Agreement
SOFTWARE LICENSE AGREEMENT
IMPORTANT - READ CAREFULLY:
THIS SOFTWARE LICENSE AGREEMENT ("Agreement") is a legal agreement between you (either an individual or a single entity) and Kingston Technology Company Inc. ("Kingston"). This Agreement relates to the software accompanying this Agreement, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation (the "Licensed Software"). By downloading, installing, copying, or otherwise using the Licensed Software, you agree to be bound by the terms of this Agreement and further agree that the third party licensors of Kingston providing licenses for all
Accept
Decline
Cancel
Next

Figure 3.1 – License Agreement

2. Create a password to protect your data on the DC. Enter it in the 'Password' field, then re-enter it in the 'Password Confirmation' field as seen below in ***Figure 3.2***. the password you create must meet the following criteria before the initialization process will allow you to continue:

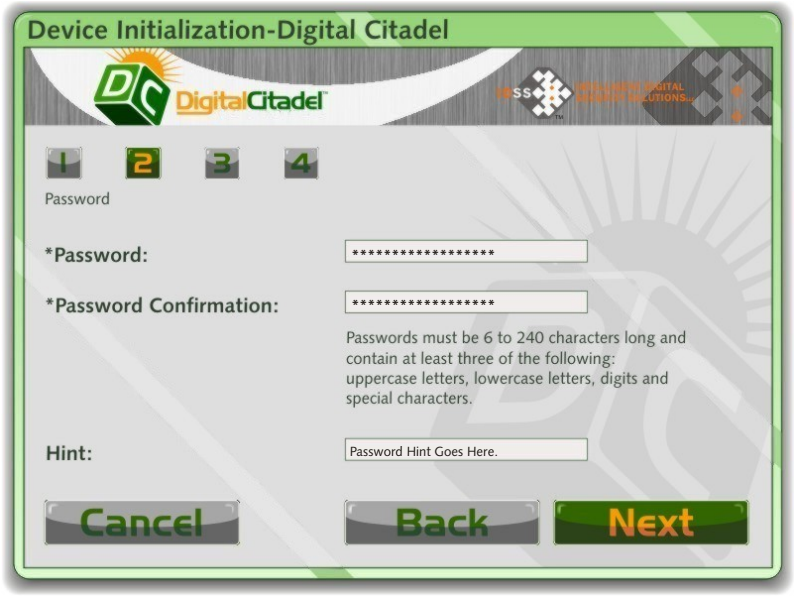

Figure 3.2 – Password Setup

- Passwords must contain 6 characters, we recommend passwords of 6-240
- Passwords must contain (3) of the following criteria options:
  - UPPER CASE, lowercase, numeric and/or special characters (!, $, etc.)

You may also enter a password hint, but it is not a mandatory field. The hint field can be useful in providing a clue as to what the password is, should the password ever be forgotten. (Note: The hint CANNOT be an exact match to the password!)

3. Enter your contact information into the text boxes provided (see ***Figure 3.3***). (Note: the information you enter in these fields may NOT contain the password string you created in Step 3. However, these fields are optional and can be left blank, if so desired.)
   - The 'Name' field may contain up to 32 characters, but cannot contain the **EXACT** password.

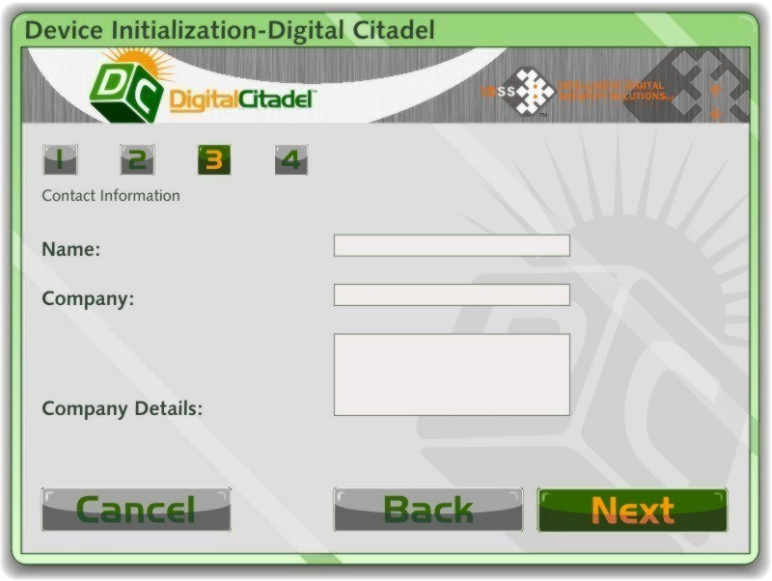

Figure 3.3 – Contact Information

- The 'Company' field may contain up to 32 characters, but cannot contain the **EXACT** password.
- The 'Details' field may contain up to 156 characters, but cannot contain the **EXACT** password.

4. Enter your authentication information into the text boxes provided (see ***Figure 3.3***). (Note: the information you enter in these fields may NOT contain the password string you created in Step 2. However, these fields are optional and can be left blank, if so desired.)

    - The 'Answer #1' field may contain up to 32 characters, but cannot contain the **EXACT** password.
    - The 'Answer #2' field may contain up to 32 characters, but cannot contain the **EXACT** password.
    - The 'Answer #3' field may contain up to 156 characters, but cannot contain the **EXACT** password.
    - The 'Email Address' field may contain up to 100 characters, but cannot contain the **EXACT** password.

Figure 3.4 – Authentication

5. Click 'Finish' to complete the device initialization process.

The **DC** will now format the secure data partition ***(Figure 3.5)*** and notify you when it is complete ***(Figure 3.6)***.

6. Click 'OK' to continue.

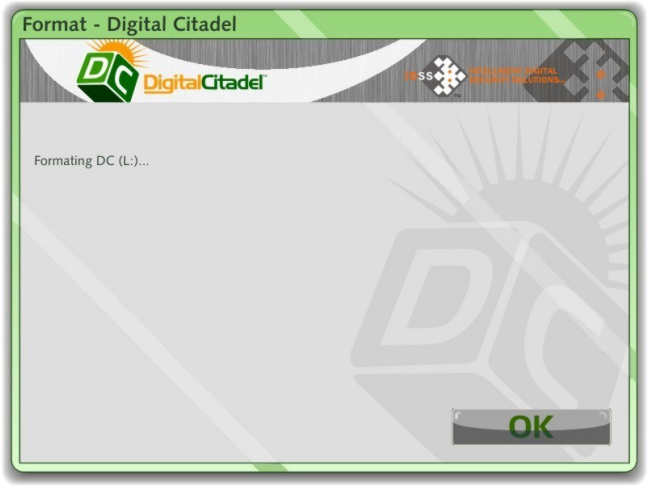

Figure 3.5 – Formatting DC

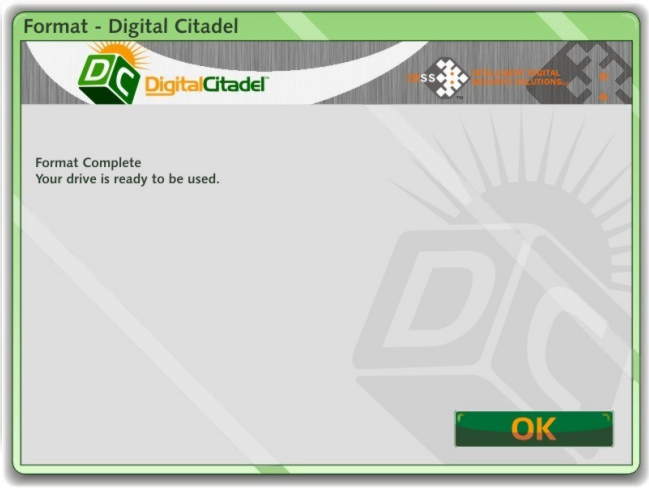

Figure 3.6 – Format Complete

Initialization complete.

*Note: Times may vary based on system hardware and the capacity of the DC drive.

Device Usage

Once the **DC** has been initialized, you can access the secure data partition and utilize the device options by logging in to the device with your password (see ***Figure 4.1***). To do so, follow these steps:

1. Insert the **DC** into an available USB port on your notebook or desktop and wait for Windows to detect it.

2. Once you've typed your email address and password, click the 'Login' button to continue.

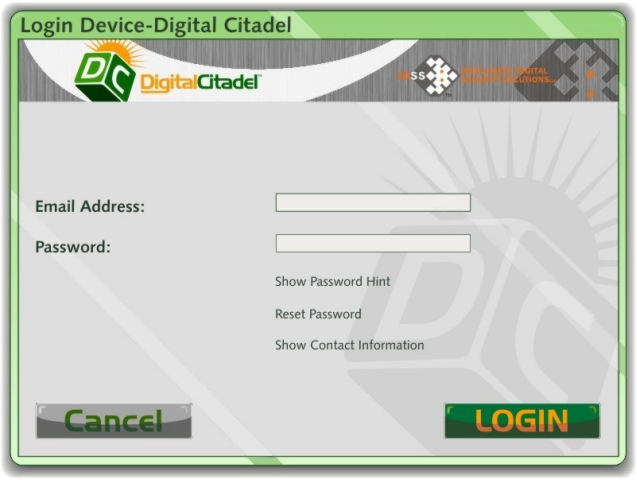

Figure 4.1 – Login Window

- If the correct email and password are entered, the **DC** will unlock and you can begin using the device.

- If an incorrect email or password is entered, an error message will appear just below the 'Hint' field, indicating a login failure (see ***Figure 4.2***).

During the login process, if a bad email address and/or password is entered, you will be given another opportunity to enter the correct password; however, there is a built-in security feature that tracks the number of failed login attempts*. If this number reaches the pre-configured value of 10 failed attempts, the **DC** will lock and require a device format of the secure data partition prior to next use.

THIS MEANS THAT ALL DATA STORED ON THE DC WILL BE LOST.

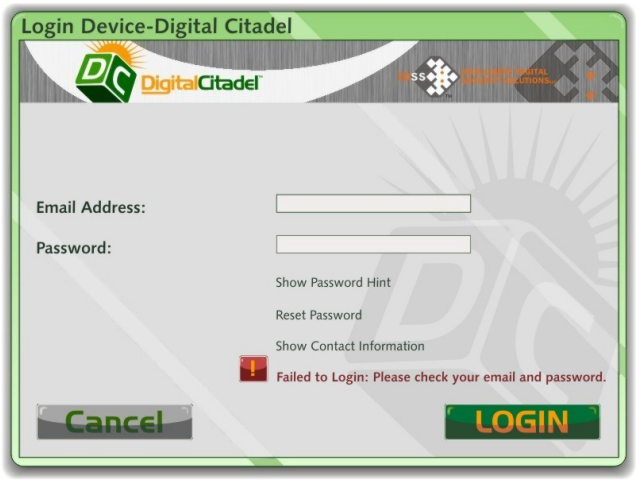

Figure 4.2 – Login Failure

*Note: Once you authenticate to the device successfully, the failed login counter will reset.

Device Options

While you are logged into the device, there will be a '**DC**' icon located in the right-hand corner of the Windows taskbar (***Figure 5.1***). (Note: Windows 7/8.x users will need to click on the up-arrow button in the taskbar in order to access the '**DC**' icon (***Figure 5.2***).

Clicking once on the **DC** icon will display the following menu:

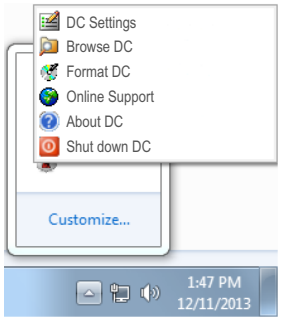

Figure 5.1 – DC icon in taskbar

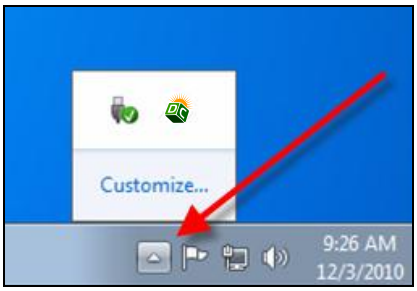

Figure 5.2 – DC icon in taskbar (Windows 7/8/8.1 users)

DC Settings

- Allows you to change your password and/or hint (***Figure 5.3***)
- Allows you to store username and password information (see **Page 11**)
- Allows you to add/view/change your contact information (***Figure 5.4***)
- Allows you to format your secure data partition (***Figure 5.5***)

(Note: For security purposes, your current **DC** password is required to update and/or modify any of these settings.)

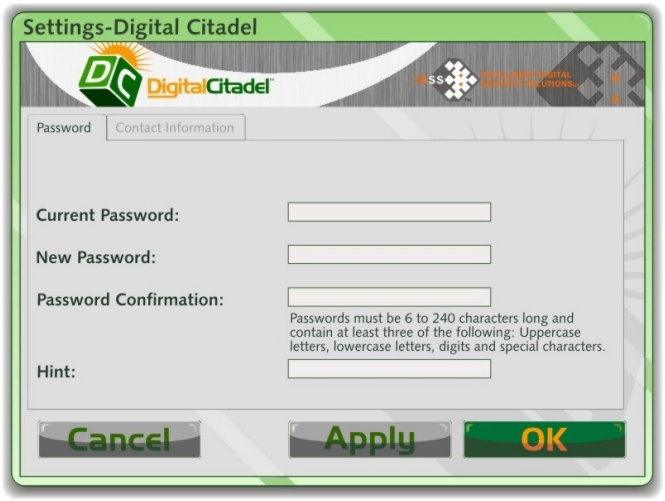

Figure 5.3 – Change Password

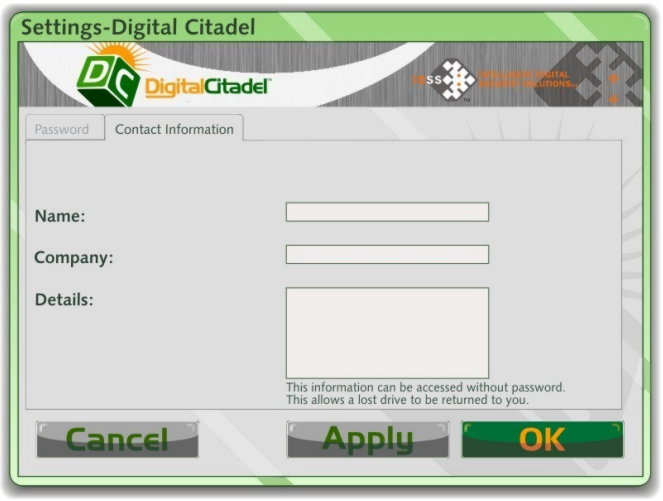

Figure 5.4 – Contact Information

Browse DC

- Allows you to browse the contents of the secure data partition while you are logged in

Format DC

- Allows you to format the secure data partition (Warning: All data will be erased.) (Figure 5.7)

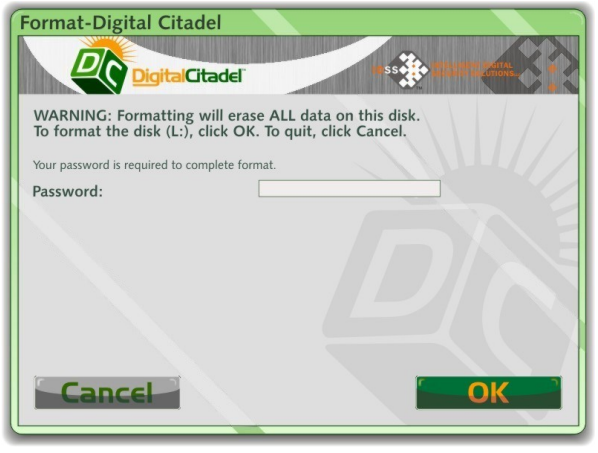
Format-Digital Citadel
DigitalCitadel
WARNING: Formatting will erase ALL data on this disk.
To format the disk (L:), click OK. To quit, click Cancel.
Your password is required to complete format.
Password:
Cancel
OK

Figure 5.5 – Format Warning

Online Support (Requires Internet Access)

- Opens your Internet browser and navigates to http://www.intelligentdigitalsecuritysolutions.com/support/ where you can access additional support information

About DC

- Provides specific details about the DC, including Application and Firmware version information (***Figure 5.7***)

Shutdown DC

- Properly shuts down the **DC**, allowing you to safely remove it from your system

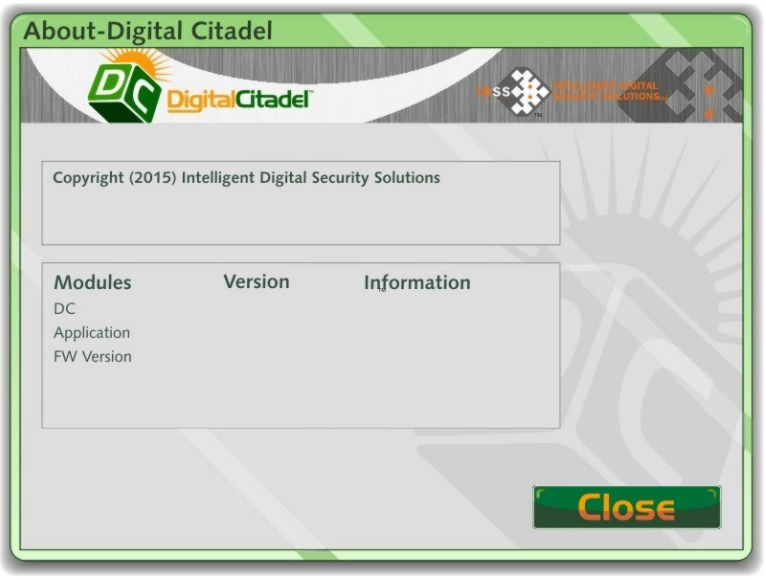

Figure 5.7 – About DC

*Note: Your current **DC** password is required in Windows Vista, Windows 7, and Win 8

Drive Letter Conflict

As mentioned in the 'System Requirements' section of this manual (on **page 3**), the **DC** requires two consecutive drive letters AFTER the last physical disk that appears before the 'gap' in drive letter assignments (see ***Figure 10.5***). This does NOT pertain to network shares because they are specific to user-profiles and not the system hardware profile itself, thus appearing available to the OS.

What this means is, Windows may assign the **DC** a drive letter that's already in use by a network share or Universal Naming Convention (UNC) path, causing a drive letter conflict. If this happens, please consult your administrator or help desk department on changing drive letter assignments in Windows Disk Management (administrator privileges required.)

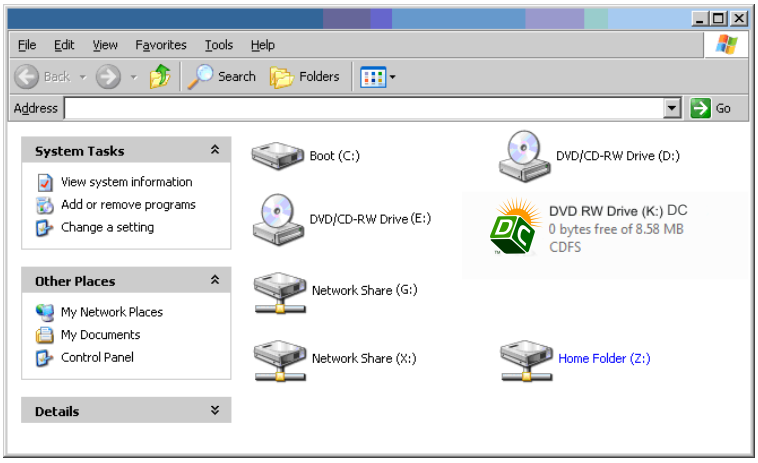

Figure 6.1 – My Computer

In this example, the **DC** uses drive F:, which is the first available drive letter after drive E: (the last physical disk before the drive letter gap.) Because letter G: is a network share and not part of the hardware profile, the **DC** may attempt to use it as its second drive letter, causing a conflict.

If there are no network shares on your system and the **DC** still won't load, it is possible that a card reader, removable disk, or other previously-installed device is holding on to a drive-letter assignment and still causing a conflict.

Please note that Drive Letter Management, or DLM, has improved significantly in Windows Vista, and 7, so you may not come across this issue, but if you are unable to resolve the conflict, please contact Intelligent Digital Security Solution's Technical Support Department for further assistance.

© 2015 Intelligent Digital Security Solutions. All rights reserved. All registered trademarks and trademarks are the property of their respective owners.